

文章编号:1001-9081(2009)08-2200-04

高级数据加密标准的差分电磁分析

丁国良,李志祥,尹文龙,赵 强

(军械工程学院 计算机工程系,石家庄 050003)

(DGL998@163.com)

摘 要:为研究高级数据加密标准(AES)针对电磁旁路攻击的脆弱性,分析了微处理器的电磁信息泄漏模型和攻击 AES 时 D 函数的选择问题。针对 PHILIPS 89C51 实现的 AES-128 密码系统,采用差分电磁分析的方法进行了密码破译实验,成功获得了 128 位密钥。经分析发现 AES 的字节替代变换可产生密钥泄露,为密码系统实施相关防护措施提供了依据。

关键词:差分电磁分析;电磁信息泄漏;高级数据加密标准;旁路攻击

中图分类号:TP309.7 **文献标志码:**A

Differential electromagnetic analysis on advanced encryption standard (AES)

DING Guo-liang, LI Zhi-xiang, YING Wen-long, ZHAO Qiang

(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang Hebei 050003, China)

Abstract: To study the vulnerability of Advanced Encryption Standard (AES) against electromagnetic side channel attacks, the article analyzed the electromagnetic information leakage model of microcomputer and the choice of D function. Then, concerning the AES-128 bits cryptographic system realized by the 89C51 microchip, Differential Electromagnetic Analysis (DEMA) algorithm, which was used into an attack experiment and succeeded in obtaining 128 bits secret key of AES-128, was described. After analyzing the experimental results, the leakage of secret information produced by ByteSub transformation was detected. This method can be regarded as a new protective measure in cryptographic systems.

Key words: Differential ElectroMagnetic Analysis (DEMA); electromagnetic information leakage; Advanced Encryption Standard (AES); Side Channel Attack (SCA)

0 引言

2001 年 11 月,美国国家标准和技术研究所(NIST)宣布 Rijndael 算法成为新的数据加密标准——高级数据加密标准(Advanced Encryption Standard, AES),并将逐渐取代数据加密标准(Digital Encryption Standard, DES)而广泛应用于通信和信息系统安全领域^[1]。在 Rijndael 算法中,最主要的设计指标就是具有强的抗差分分析能力,因此被认为是安全性最高的对称分组加密算法。目前针对 AES 的密码分析主要集中在积分分析、代数攻击和功耗分析三个方向^[2-3]。前两种方法是传统分析方法,主要是从 AES 算法的设计角度分析算法的数学结构,附以关于算法输入/输出的某些假设,结合统计测试进行密码分析;而后者是利用算法实现中的漏洞,通过分析密码算法在运行过程中的功耗变化而得到密钥。这种技术称之为旁路攻击或侧信道攻击(Side Channel Attack, SCA),具有很强的攻击能力,自 1999 年 Paul Kocher 等人成功用于攻击 DES 之后^[4],就引起业内人士的广泛关注。

SCA 主要包括计时攻击、功耗攻击和电磁攻击等^[5]。随着近年来对电磁信息泄漏的研究,人们发现电磁辐射泄漏的信息不仅丰富,而且在攻击时无需分解设备和改动电路,具有很强的实用性。本文针对 AES 密码系统,利用 CMOS 集成电路产生的电磁辐射信号,采用差分电磁分析的方法,在 500 组

样本量的情况下,用时约 30 min 获得了 AES-128 的全部密钥。实验结果表明,AES 在字节替代运算处存在信息泄漏,未加防护的 AES 算法在电磁分析面前是脆弱的,与传统分析方法相比,SCA 具有很强的攻击能力。

1 电磁辐射与数据相关性

目前大规模数字集成电路主要由 CMOS 门电路实现。在 CMOS 器件中,操作对象为数字信号,所有操作都是在时钟的控制下进行,每个时钟上升沿或下降沿触发各部件动作,使之逻辑状态产生变化。

以 CMOS 反向器为例,典型的输入和输出电压波形以及负载电容电流波形如图 1 所示。由于数字集成电路芯片的开关特性,其工作电流一般为瞬态脉冲电流形式。电流的大小是输出电压的一个函数^[6],可表示为:

$$i_c = i_{D,p} - i_{D,n} = C_L \frac{dV_{out}}{dt}。$$

根据电磁场理论,时变电流是产生辐射电磁场的源。因此,数字集成电路在工作状态下会产生大量的电磁辐射信号,特别是与数据操作有关的控制器、运算器、存储器和总线等部件,这些部件在时钟周期控制下,其状态变化取决于运算、操作对象以及运算结果,这些状态信息和电磁辐射信号之间存在着一定的联系。利用这种相关性,通过分析两者之间的关

收稿日期:2009-02-19;修回日期:2009-04-17。

基金项目:国家 863 计划项目(2007AA01Z454);国家自然科学基金资助项目(60571037)。

作者简介:丁国良(1968-),男,江苏张家港人,副教授,硕士,主要研究方向:嵌入式系统、信息安全;李志祥(1982-),男,山东济南人,助教,硕士,主要研究方向:信息安全;尹文龙(1980-),男,河北石家庄人,讲师,硕士,主要研究方向:嵌入式系统;赵强(1945-),男,吉林长春人,教授,主要研究方向:集成电路安全防护。

系,就可能获得其中的数据,从而造成敏感信息的泄漏。

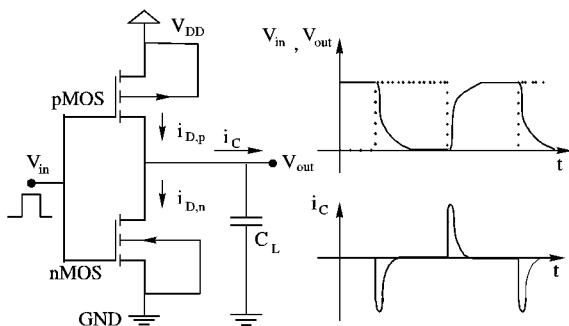


图1 CMOS反相器开关过程输入输出电压和电容电流波形

2 电磁信息泄漏模型

文献[7]对于动态 CMOS 门电路的能耗提出汉明重量模型。动态 CMOS 门电路的能耗与其当前状态有直接关系,通常 CMOS 门电路处于高电平状态时有能耗,低电平则无能耗,可用汉明重量描述,即 $E = aHw(x) + b$ 。其中, E 表示电能消耗, x 表示 CMOS 门所处的状态, $Hw(x)$ 为 x 的汉明重量, a 为汉明重量与电能消耗间的比例系数, b 为与所处理数据不相关的电能消耗及噪声。由于电磁辐射能量是整个 CMOS 门电路能耗的重要体现,且与之成正比,因此可将这个功耗模型推广至电磁辐射模型。

目前的微控制器一般都是采用 CMOS 工艺实现。指令是微处理器完成数据运算的基本操作,每一个指令会涉及到多个基本单元,例如 MOVX A @DPTR 指令。在该指令执行期间,会有 PC、PSW、IR、ACC、存储器单元以及总线等多个基本单元的状态发生变化,其中涉及数据的单元有 ACC、存储器和总线等,这些单元由于状态发生变化会产生电磁辐射,从而存在信息泄漏的可能。对于 ACC 和存储器单元,由于这些单元的功能主要是保存数据或参与运算,在数据操作期间保存在其中的原始数据不会受到其他数据的影响,因而用寄存器级的汉明重量模型预测或仿真微控制器中基本单元的电磁辐射能量是合适的。

引理 1 对于 n 位处理器, n 位寄存器或存储器单元 D 的数值记为 $D = \sum_{i=0}^{n-1} d_i 2^i, d_i \in \{0,1\}$, 则其汉明重量可记为 $Hw(D) = \sum_{i=0}^{n-1} d_i, d_i \in \{0,1\}$, 其中 d_i 为寄存器 D 中第 $i+1$ 位的值。

定义 1 对于寄存器或存储器单元 D 在一次运算过程中产生的电磁辐射能量,可用运算结果 D 的汉明重量描述,其能量大小可表示为 $E = aHw(D) + b$ 。

从总线的物理结构看,总线连接 ALU、存储器和控制器等多个部件,具有很长的传输线,因此一般采用预充电技术设计^[7]。总线在无数数据传输时进行预充电,并保持在高电平状态,而当数据送至总线或端口后,数据等于 1 的总线位状态不变,而等于 0 的位通过放电变为低电平。因此,总线每次数据传输所产生的电磁辐射能量主要决于数据中 0 的位数,其汉明重量模型可以按下述定义描述。

引理 2 对于 n 位处理器, n 位宽度的总线 Bus 的数值记为 $B = \sum_{i=0}^{n-1} d_i 2^i, d_i \in \{0,1\}$, 则其汉明重量可记为 $Hw(B) = \sum_{i=0}^{n-1} d_i, d_i \in \{0,1\}$, 其中 d_i 为总线 Bus 中第 $i+1$ 位的值。

定义 2 对于 n 位宽度的总线 Bus 在一次数据传输过程中产生的电磁辐射能量,可用传送数据的汉明重量描述,其能量大小可表示为 $E = a(n - Hw(Bus)) + b$ 。

3 AES 的差分电磁分析

差分电磁分析的基本原理是由于在加密过程中芯片工作要产生电磁辐射,而辐射能量的大小随处理的数据不同会有微小的变化,对这种变化采用差分方法可以确定所处理的数据是 0 还是 1,从而有可能猜出加密算法中所使用的密钥。

3.1 基本原理

差分电磁分析是基于假设检验理论的一种统计方法,最初由 Paul Kocher 用于 DES 差分功耗分析^[4]。其分析过程是首先构造一个 D 函数。构造方法是选择一个在加密过程中与密钥相关的运算 $F(PT_i, K_b) = CT_i$, 其中 $F()$ 是加密过程中的某一确定函数, PT_i 为已知的函数输入, CT_i 为函数输出, K_b 为被猜测的密钥。如果根据已知明文猜测密钥,则可直接将 $F()$ 作为 D 函数, CT_i 作为 D 值;如果根据已知密文猜测密钥,则根据 $F()$ 的逆运算得到 D 函数 $D(CT_i, K_b) = PT_i, PT_i$ 作为 D 值,因此 D 函数可统一记为 $D = D(PT_i | CT_i, K_b), D \in \{1,0\}$ 。攻击时,把 $D \in \{1,0\}$ 作为一个判别函数,根据被猜测的密钥 K_b 与已知的 CT_i 或 PT_i 计算得到 D 值,将采集到的信号曲线根据 D 值是 1 还是 0 分成两组,并作差分。因为只有根据猜测正确密钥 K_b 计算的 D 值才正确,由于计算 1 和 0 的产生的功耗不同,两组差分后就会产生明显的尖峰,而其他错误猜测值的差分曲线则不会产生尖峰,由此可以根据是否存在尖峰而判断猜测的密钥值是否正确。

3.2 D 函数的构造

D 函数构造因具体的加密算法而异,但必须是已知量和密钥 K 的函数。AES 算法是一个使用可变分组和密钥长度的迭代分组密码,以 AES-128 为例,它的轮函数是由三个不同的可逆一致变换组成:非线性 S 盒置换、线性扩散和轮密钥加,分别由 ByteSub(字节替代)、ShiftRow(行移位)、MixColumn(混合列)、AddRoundKey(轮密钥加)4 个运算实现。在这 4 个运算中选择合适的函数构造为 D 函数是差分电磁分析成功的关键。

首先选择第一轮的轮密钥加运算的输出作为 D 函数。AES 轮密钥加运算的实质上是明文和密钥的异或操作,可以描述为 $PT \oplus K$, 这里涉及到已知的明文和需要猜测的密钥,可以作为 D 函数,可描述为 $D = PT_{ik}^1 \oplus K_k^1, D \in \{0,1\}$, 其中 PT_{ik}^1 表示第 i 个明文中第 $k(k \in \{1, \dots, 16\})$ 个字节的 1 位, K_k^1 表示被攻击密钥的第 $k(k \in \{1, \dots, 16\})$ 个子密钥中的 1 位, K_k 猜测值的范围为 0~255。经分析发现,若 $K_k^1 = 0$, 则有 $D = PT_{ik}^1$, 因而根据 D 的值划分两个集合 $Set_{0m} = \{S_{ij} | PT_{ik}^1 = 0\}$ 和 $Set_{1m} = \{S_{ij} | PT_{ik}^1 = 1\}$; 若 $K_m^1 = 1$, 则有 $D = NOT(PT_{ik}^1)$, 进而得到两个集合 $Set_{0m}^* = \{S_{ij} | PT_{ik}^1 = 1\}$ 和 $Set_{1m}^* = \{S_{ij} | PT_{ik}^1 = 0\}$ 。注意到这两组集合存在着相等关系 $Set_{0m} = Set_{1m}^*$ 和 $Set_{1m} = Set_{0m}^*$ 。所以对任意的明文,曲线分组只有两种形式,且两者只有正负符号不同,不可能判断出哪个密钥是正确的,因而 1 位的轮密钥加运算不宜作为 D 函数。

字节替代是 AES 算法中唯一的非线性置换运算,它利用 S 盒独立作用于状态中的每一个字节,其输出可描述为 $SBox(State \oplus EK)$, 其中 $State \oplus EK$ 为初始或上一轮密钥加

运算的输出, EK 为扩展密钥。由于字节替代的非线性, S 盒每一位的输出不仅对 $State$ 和 EK 中的对应位敏感, 而且对输入的其他位的变化也非常敏感, 这就保证了由正确密钥和错误密钥计算出来的 D 值相对独立, 也就是降低了由错误密钥计算的预测值与实测电磁辐射能量之间的相关性, 从而容易从差分曲线中辨别出正确的密钥。因此, 本文采用 AES 第一轮字节替代变换的 S 盒输出作为 D 函数。第一轮 S 盒输出表达式中的 $State$ 就是明文, EK 就是密钥, D 函数可表示为 $D = SBox(PT_{ik}^1 \oplus K_k^1)$, $D \in \{0, 1\}$ 。

3.3 差分电磁分析算法

当进行差分分析时, 首先需要进行 M 次加密运算, 经采样获取 M 条电磁辐射信号曲线以及相应的 M 个随机的明文。针对 AES-128 攻击的 DEMA 算法如下:

输入: 1) $PT[i]$ ($1 \leq i \leq M$): M 组随机明文;
2) M : 加密次数;
3) N : 每条电磁辐射信号的采样点数;
4) $S[i][j]$ ($1 \leq i \leq M, 1 \leq j \leq N$): 采集的电磁辐射信号;
5) b : 被攻击的子密钥的位数, $b = 8$ 。

输出: 正确子密钥。

```
for k from 0 to  $2^b - 1$  do
  for j from 0 to  $N - 1$  do
     $p = 0; q = 0; A0[j] = 0; A1[j] = 0;$ 
    for i from 0 to  $M - 1$  do
      if  $D(PT[i], k) = 0$  then
         $A0[j] = A0[j] + S[i][j];$ 
         $p = p + 1;$ 
      else
         $A1[j] = A1[j] + S[i][j];$ 
         $q = q + 1;$ 
      end if
    end for
     $\Delta[k][j] = A0[j]/p - A1[j]/q;$ 
  end for
end for
Return:  $\Delta[k][j]$  最大峰值的  $k$ ;
```

在 AES-128 所有的 16 个子密钥猜测完成后, 128 位密钥就可以获得。

3.4 算法的计算复杂度分析

假设加密次数为 M , 每条电磁辐射信号的采样点数为 N 。算法共有三个 for 循环嵌套, 第一个 for 循环的次数为 2^b , 第二个 for 循环的次数为 N , 第三个 for 循环的次数为 M , 因此该算法的时间复杂度为 $O(2^b MN)$ 。由此可以看出当 M, N 一定时, 时间复杂度随着 b 的增加成指数级增长。但由于该算法采用“分而治之”的思想, 把 128 位密钥分成 16 个子密钥, 每一个子密钥有 8 位, 即 $b = 8$, 因此对 8 位子密钥进行猜测时, 时间复杂度可以认为是 $O(MN)$, 因此完成 128 位的密钥猜测时的时间大大降低。

与其他攻击方法相比, 代数攻击采用 MQ (overdefined Multivariate Quadratic system) 方法对 AES-128 可构造出 8 000 个含有 1 600 个变量的二次方程组成的代数方程系统, 直接采用 XL (eXtended Linearization) 方法求解其攻击复杂度为 2^{330} , 而采用 XSL (eXtended Sparse Linearization) 方法的复杂度为 $2^{230[8]}$, 因此运算量非常巨大, 导致分析非常困难。积分分析是 AES 最有效的攻击方法之一, 现阶段 1 阶积分分析只是从

理论上突破了 4 轮至 6 轮的简化 AES, 而高阶积分分析对更高轮次的 AES 算法的攻击能力是否有效还在探索之中^[1,9]。由此可见, 差分电磁分析在时间复杂度上具有极大的优势, 可以在极短的时间内获得 AES 的全部密码, 这在后面的攻击实验中得到了证实。

4 实验及结果分析

本实验攻击的对象为 PHILIPS 89C51 单片机构成的最小系统, 其上运行 AES-128 加密算法。电磁辐射信号采集传感器采用的 Langer EMV-Technik 公司的近场探头 RF-R400-1, 测量时水平放置于被测 CPU 上方约 0.5 cm 处, 数据采集装置为泰克 DPO4104 存储式数字示波器, 采样深度设置为 10 000 点, 采样率 250 MSa/s。整个信号采集、控制及分析均在 PC 机的控制下完成。实验装置如图 2 所示。

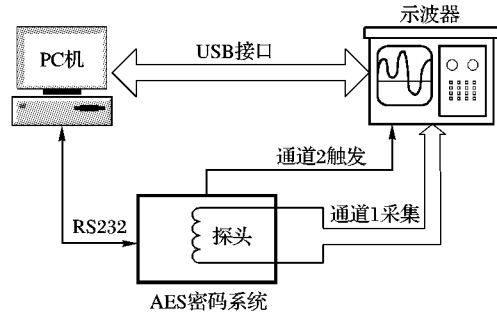


图2 DEMA 攻击实验平台示意图

攻击时, PC 机随机生成 M 组 128 位二进制明文, 通过串口传至 AES-128 密码系统, 密码系统收到明文后运行加密程序对明文进行加密。同时触发示波器开始数据采集, 示波器通过近场探头 RF-R400-1 采集电磁辐射信号并保存在自身的存储器中, 采样完成后通过 USB 总线将数据上传至 PC, 最后密码系统将加密产生的 128 位二进制密文传送至 PC 机。PC 机在整个攻击过程中共获得 M 组一一对应的明文、密文和在加密过程中采集的电磁辐射信号。

分析时, 首先采用总线的汉明重量模型, 取 AES 第一轮 S 盒的输出为 D 函数, 对采集的 500 组电磁辐射信号进行差分电磁分析。当猜测第一个子密钥为 112 时, 差分曲线有明显的尖峰, 攻击效果如图 3 所示。而其他猜测值时无明显尖峰, 这说明 112 为正确密钥。

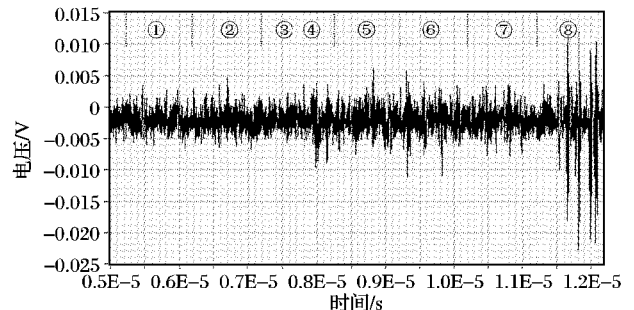


图3 DEMA 攻击效果图

通过分析被攻击的程序得知, 不同的指令具有不同的电磁泄露特征。实验中的 AES 采用 C 语言编写, 并利用 Keil51 集成开发环境编译成机器代码。下面的程序为 AES 第一轮的轮密钥加变换和字节替代变换的实现过程, 该操作经编译变成 8 条机器指令, 图 3 中带圈数字表示对应的机器指令在差分曲线中的位置。

① MOV DPTR, #state(0x00B9)

```

② MOVX    A, @DPTR
③ MOV      RO, #key(0x44)
④ XRL      A, @RO
⑤ MOV      DPTR, #sbox(0x0026)
⑥ MOVC     A, @A + DPTR
⑦ MOV      DPTR, #state(0x00B9)
⑧ MOVX     @DPTR, A

```

指令①~④实现轮密钥加变换:首先指令①和②是把明文从外部数据存储器存入寄存器A,指令③取密钥在内部存储器中的地址送入R0,最后指令④实现明文与密钥的异或运算。指令⑤~⑧实现字节替代变换:指令⑤取S盒查找表的首地址,指令⑥以轮密钥加的结果为偏移量,从外部ROM的S盒查找表中取出替换字节,指令⑦⑧把结果存入到外部RAM中。

由图3可以看出,数据相关性最强即尖峰幅度最大的点位于指令⑧执行期间,指令MOVX是将替换结果通过总线传输并保存在外部RAM中,而传输的数据正是攻击的D函数的值,从而这也验证了对总线泄漏原因分析及模型的正确性。除此之外,指令⑥的峰值相对较大,该指令实现查找表功能,是将替换结果从外部ROM通过总线传送到ACC寄存器,ACC的内容也是攻击的D函数的值,但不同的是攻击的目标保存到了寄存器中。由此可以认为AES算法的S盒输出存在信息泄漏,而写入外部RAM的MOVX指令泄漏的密钥信息最大,其次为传送到ACC的MOVC指令。图3是分析AES-128位密钥第1个字节的电磁信号差分结果,其他15个字节可以同样方法获得。实验证实仅用500个样本即可分析出AES-128全部的密钥,时间约30 min。

除此之外,实验还采用了寄存器级的汉明重量模型对同一组数据进行了分析,获得了与图3相似的图形。这是由于两者攻击的对象都是S盒的输出,对于实测数据的分组应是一致的,因此差分出的曲线是一样的。从图3中可以看出总线产生的电磁信息泄漏要比寄存器大,从电路结构上分析产生这种现象的原因是由于总线采用预充电技术,总线与其他部件相比具有更大的寄生电容,这些电容在充放电时产生的电磁辐射能量更大,因此更容易产生信息泄漏。

5 结语

本文采用DEMA方法把对AES-128密钥的搜索空间从 2^{128} 降至 $2^8 \times 16 = 4096$,极大地缩小了穷举搜索的密钥空间,

可在短时间内分析出AES-128的密钥,证实了AES软件实现面对旁路攻击时的脆弱性。通过分析AES程序可以看到,AES最可能产生信息泄漏的运算是字节替代变换。此外,不同的指令具有不同的电磁辐射特征,泄漏最严重的指令是将S盒输出写入外部RAM的MOVX,其次是从S盒查找表读入数据的MOVC指令。本文实验结果表明,微处理器在工作期间会产生电磁信息泄漏,采集这些电磁辐射信号并通过统计分析,可以获得运算过程中的敏感信息,因此,针对此类攻击手段及其防御措施的研究均应引起足够重视。

参考文献:

- [1] DAEMEN J, RIJMEN V. AES proposal: Rijndael(Version 2)[EB/OL]. [2009-02-01]. <http://csrc.nist.gov/encryption/aes>.
- [2] 肖国镇,白恩健,刘晓娟. AES密码分析的若干新进展[J]. 电子学报, 2003, 31(10): 1549-1554.
- [3] TILLICH S, HERBST C. Attacking state-of-the-art software countermeasures — A case study for AES[C]// Proceedings of the 10th International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 5154. Berlin: Springer, 2008: 228-243.
- [4] KOCHER P, JAFFE J, JUN B. Differential power analysis[C]// Advances in Cryptology — Proceedings of Crypto. Berlin: Springer, 1999: 388-397.
- [5] AGRAWAL D, ARCHAMBEAULT B, RAO J R, et al. The EM side-channel(s): Attacks and assessment methodologies[C]// Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 2779. Berlin: Springer, 2003: 29-45.
- [6] KANG S-M, LEBLEBICI Y. CMOS 数字集成电路分析与设计[M]. 3版. 王志功, 窦建华, 译. 北京: 电子工业出版社, 2005: 194.
- [7] MESSERGES T S, DABBISH E A, SLOAN R H. Investigation of power analysis attacks on smartcards[C]// Proceedings of the USENIX Workshop on Smartcard Technology, 1999. Berkeley, CA, USA: USENIX Association, 1999: 151.
- [8] COURTOIS N, PIEPRZYK J. Cryptanalysis of block ciphers with over defined systems of equations[DB/OL]. [2009-02-01]. <http://www.iscr.org>.
- [9] FERGUSON N, KELSEY J, LUCKS S, et al. Improved cryptanalysis of Rijndael[C]// 7th International Workshop on Fast Software Encryption: FSE 2000. New York, USA: Springer-Verlag, 2001: 213-230.

(上接第2199页)

软件实现方面:基于位的LFSR软件实现效率低下,本文选用的 σ -LFSR不仅具有良好的伪随机性,也非常适合软件快速实现,用计算机的基本指令循环移位和与操作即可实现。

由于算法只是对S盒次序进行重组,而不增加分组长度,不产生新的S盒,因此软件、硬件开销都很小,并且几乎不增加运算时间。

参考文献:

- [1] 冯登国,吴文玲. 分组密码的设计与分析[M]. 北京: 清华大学出版社, 2000: 67-69.
- [2] BIHAM E, BIRYUKOV A. How to strengthen DES using existing hardware[C]// Advances in Cryptology — ASIACRYPT '94. Berlin: Springer-Verlag, 1994: 398-412.

- [3] O'CONNOR L. Enumerating nondegenerate permutations[C]// Proceedings of Advances in Cryptology EUROCRYPT '93. Berlin: Springer-Verlag, 1993: 368-377.
- [4] 卢开澄. 计算机密码学[M]. 北京: 清华大学出版社, 2002: 72-74.
- [5] HEYS H M, TAVARES S E. The design of substitution-permutation networks resistant to differential and linear cryptanalysis[C]// Proceedings of 2nd ACM Conference on Computer and Communications Security. New York: ACM, 1994: 148-155.
- [6] 曾光,何开成,韩文报. 一类三项式形式适合软件实现的 σ -LFSR[J]. 中国科学: E辑(信息科学), 2007, 37(2): 209-222.
- [7] MERKLE R C, HELLMAN M E. On the security of multiple encryption[J]. Communications of the ACM, 1981, 24(7): 465-467.